Volume I, Chapter 2 – Table of Contents

This page intentionally left blank.

2. Network Infrastructure Requirements

The ITI must provide the underlying information transport and service networks for addressing the diverse operational requirements of the DON. This can be summarized as the capability to deliver accurate and timely information in the appropriate form to the intended recipients in a secure and cost-effective manner.

The ITI provides communication and information distribution capabilities to the DON and to its extended external user communities and locations. The magnitude of these required capabilities is difficult to accurately predict, given the rapidly changing demands and opportunities for leveraging IT for enterprise transformation. Therefore, a general requirement of the IT network infrastructure architecture is that it be flexible and scaleable in order to meet the expected rapid but unpredictable growth in all aspects.

The ITI for the DON must also support a wide variety of specific user requirements. The DON Board of Representatives established the requirement that the enterprise network architecture address tactical and non-tactical, afloat and ashore, Navy and Marine Corps applications. There are significant challenges (geographical, organizational, mobility, security, operational, budgetary, and technical) that must be specifically addressed and accommodated. Perhaps the most challenging is to support the myriad autonomous networks and communities of interest that currently operate within the DON and begin merging these into an integrated enterprise network capability.

The following is a list of DON ITI requirements organized according to the Network Architecture Framework. These requirements have been collected into a single chapter to provide a consolidated reference for the architectural solutions that follow in the remainder of the document.

2.1 Operational Requirements

The following lists represent general requirements of the operational capabilities of the DON IT network infrastructure.

2.1.1 All Communities of Users

The DON IT network infrastructure must meet the communication and connectivity needs of all parties involved in fulfilling the mission of the DON, including the following user communities:

- All commands, functions, and task groups within the DON
- Joint forces
- Allied forces
- Reserves
- Contractors
- Intelligence community
- Recruits
- Other government agencies
- Foreign governments
- Academic/research community
- Medical community
- General public
- Other stakeholders

2.1.2 All Operating Areas

The DON IT network infrastructure must meet these communication and connectivity needs in all operational areas and environments in an efficient and secure manner, including:

- CONUS bases and facilities of all types
- OCONUS bases and facilities of all types
- Battle Groups and ships at sea and in port
- Expeditionary forces at sea and on the ground
- Squadrons and planes on base, on ship, and in the air
- Any facilities, equipment, or personnel deployed in space
- Remote access for mobile users
- Access to and from contractor sites
- Access to and from telecommuting and home locations
- CONUS and globally-distributed functions and teams

2.1.3 All Types of Media

With ongoing advances in digital networking, the DON IT network infrastructure is expected to support all types and forms of information transport in secure and non-secure transmissions, including:

- Data , including numeric, text, graphics, and images
- Voice
- Video
- Multi-media
- Non-POTS telephony services (mobile, cellular, and radio frequency), digital telephony, voice mail, computer-integrated telephony, interactive voice response, single-line concept, and enhanced 911
- Paging

2.1.4 All Types of Application Networking Requirements

There are many different types of systems that do or will depend upon the DON IT network infrastructure for meeting their communication requirements. There are networking requirements for data gathering, online access for users, inter-application information exchange, and the use of the network for distributed database access. These networking requirements for applications include:

- Information system application communications for all communities
- Support for the Global Command and Control System (GCCS) and the Global Combat Support System (GCSS)
- Support for the common tactical picture

- Support for damage control information (both conventionally, i.e. detecting damage inside a ship, and in a wider sense, i.e. detecting a chemical plume to establish decontamination boundaries)
- Support for sensor-to-shooter (especially important for Marines with a decreased footprint ashore who rely increasingly on offshore shooting assets for artillery support)
- Support for distributed combat systems such as TBM Defense
- Support for facility monitoring and control systems
- Network capacity to support data warehousing and data mining
- Supports quality of life for our sailors and Marines
- Support for approved legacy protocols consistent with ITSG
- Support for migration from legacy to adopted protocols
- Support for access to information/data maintained at and provided by non-government sites
- Phased support for force coordination, force control and critical support, and weapons control and systems control and monitoring
- Guidance and support for application planners and developers on designing for effective use of network capabilities
- Supports Y2K compliance

2.1.5 Customized Services to Meet Customer Needs

Various organizations and user communities have the requirement to establish autonomous or virtual networks within the DON IT network infrastructure. These autonomous or virtual networks must support the organizations' and communities' special needs for security, performance, and functionality.

The planning, design, and provisioning of enterprise networking services must provide the flexibility to customize services to meet specific customer needs. In order to leverage economies of scale and provide a standardized and dependable global infrastructure for all user communities, it is recommended that a common set of basic services be provided across the enterprise. The definition of basic and optional services is provided below.

- **Basic Services:** Those services defined as containing the aspects of a utility, including essential need, benefit from sharing, generic in nature, specificity not essential for individual requirements, subject to economies of scale, and can be reliably provided to many. Also includes services that should be regulated for some reason, including price, quality of service, safety, security, required investment, and law or policy.
- **Optional Services:** Those services that contain the aspects of uniqueness, individuality, or tailoring needed to meet specific needs and requirements of customers. These are services that a significant portion of the customer base does not regard as "basic" or "utility" services or capabilities.

The resulting package of network services and service levels will be established through the use of Customer Service Level Agreements. These agreements define the nature of associated use and performance measurements and will be linked to pricing and billing arrangements for each customer of the IT infrastructure.

2.1.6 Operational and Management Support Capabilities

Network customers and users require the following ongoing operational and management support capabilities from the Infrastructure Service Provider(s) which must be supported by the IT network infrastructure.

- Efficient and responsive service ordering and provisioning
- Troubleshooting and help support for installation, set-up, and on-going operations
- Timely identification and resolution of problems
- An integrated billing system (including phone support) based on services acquired and ue of the infrastructure
- Detailed accounting for services provided
- Provision of information and the capability to collect measurements, including:
  - Service use, including peak or surge characteristics, and available capacity
  - Performance criteria (bandwidth, latency, Quality of Service)
  - Service availability and outages
  - Survivability and timely casualty restoration
  - Service performance measurements

2.1.7 Evolution to Accommodate New Technologies

The DON IT network infrastructure will be built using current technologies with acceptable and manageable technical and economic risks. The architecture and resulting choices of technology components will evolve to embrace new and emerging technologies as these are seen to offer discernible advantages to customers. The means to update and refresh the architecture guidance and resulting design specifications must be built into the operational model for ongoing planning and management of the DON IT network infrastructure. This requirement includes:

- Processes for collecting future user requirements and providing feedback to planners and developers
- Support of Advanced Concept Technology Demonstrations (ACTD) and Advanced Technology Demonstrations (ATD) involving users

2.1.8 Cost Effectiveness

Providing and operating the DON IT network infrastructure must be based on sound business case analysis and management practices to optimize the ability to meet user requirements with the associated costs. This implies:

- Application of best commercial practices
- Pricing (or costs) comparable to those in private industry
- Ability to choose service providers that can deliver the best value

- The use of the Total Cost of Ownership (TCO) approach for all cost evaluations

2.2 IT Network Infrastructure Functional Requirements

In addition to the above general requirements to support the systems and operational requirements of the DON, more specific functional requirements have been identified. These have been defined using the relevant components of the EAF for network architecture.

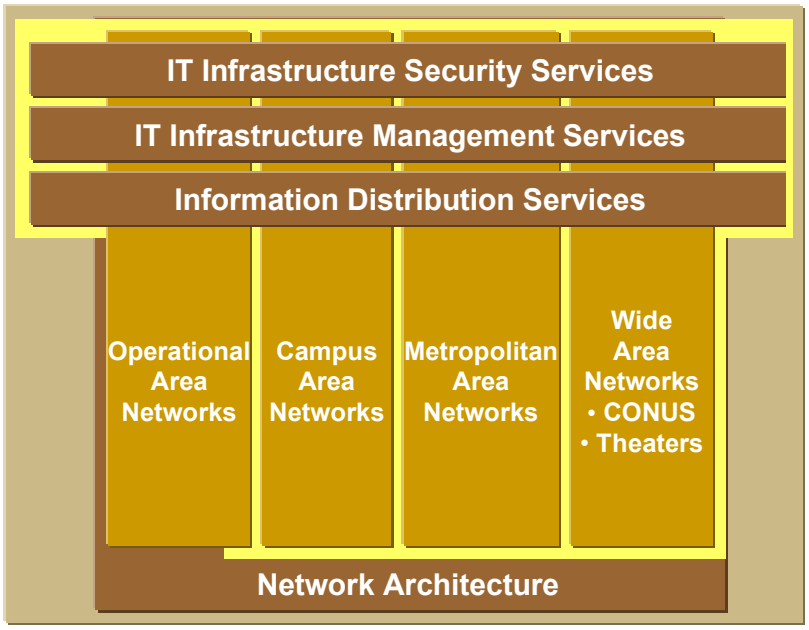

Figure 2-1. Framework for Identifying IT Network Infrastructure Requirements

The DON IT network infrastructure functional requirements are identified in the following sub-sections for each of the three service levels in this framework. Specific network connectivity requirements for each of the four classes of networks are further identified in the subsequent section.

2.2.1 IT Infrastructure Security - Functional Requirements

One of the highest priorities for DoD and DON global networks is security. There is a requirement for the DoD "Defense in Depth" program to be fully implemented in the DON. This will assure confidentiality, integrity, authentication, and non-repudiation. All security requirements must be met across all networks, including the attached clients and servers. The following detail the specific network security services that are required:

- Access control services
- Intrusion detection services
- Encryption services
- Attack shunning
- Public key administration
- Proxy services
- Vulnerability detection services
- Malicious code detection

- Illegal use detection
- Enclave protection

2.2.2 IT Infrastructure Management - Functional Requirements

There is a need for end-to-end global distributed network management. This includes the requirements for a series of integrated network operations centers. The IT infrastructure management requirements are:

- Fault management
- Performance management
- Configuration management
- Software distribution
- Help desk services
- Usage accounting management
- Capacity planning, network modeling, and trend analysis
- Asset management
- Integration management
- File management

2.2.3 Information Distribution Service - Functional Requirements

The Information Distribution Services provide IT infrastructure users with various capabilities to manage the distribution and delivery of information. These requirements are defined below. They are divided into basic and optional services.

Basic Services include:

- Network time service
- Domain name/network addressing services
- Enterprise directory services
  - Directory synchronization within the DON
  - Directory service accessibility by applications and systems
- Message transfer services
- Electronic mail (e-mail)
- E-mail attachments
- Network news service
- Web-hosting and transport services
- File transfer services
- Remote access services
- General voice (including conferencing)
- Shipboard voice
- Secure voice
- Multimedia services

Optional Distribution Services include:

- Defense Messaging System
- Facsimile transmission
- Electronic Commerce/Electronic Data Interchange (EC/EDI)
- Workgroup computing
- Electronic dialog (chat)
- Collaborative planning with imagery (groupware)
- Video Teleconferencing (VTC)
- Multi-cast broadcasting and other “many-to-many” and “one-to-many” applications
- Software distribution services
- Television broadcasting

- Software distribution services

2.3 IT Network Infrastructure Connectivity Requirements

The DON IT network infrastructure must provide end-to-end connectivity across all four network categories – operational, campus, metropolitan, and wide area. This includes connectivity to all users and operational locations as outlined above, including internal and external users/locations and remote/mobile access.

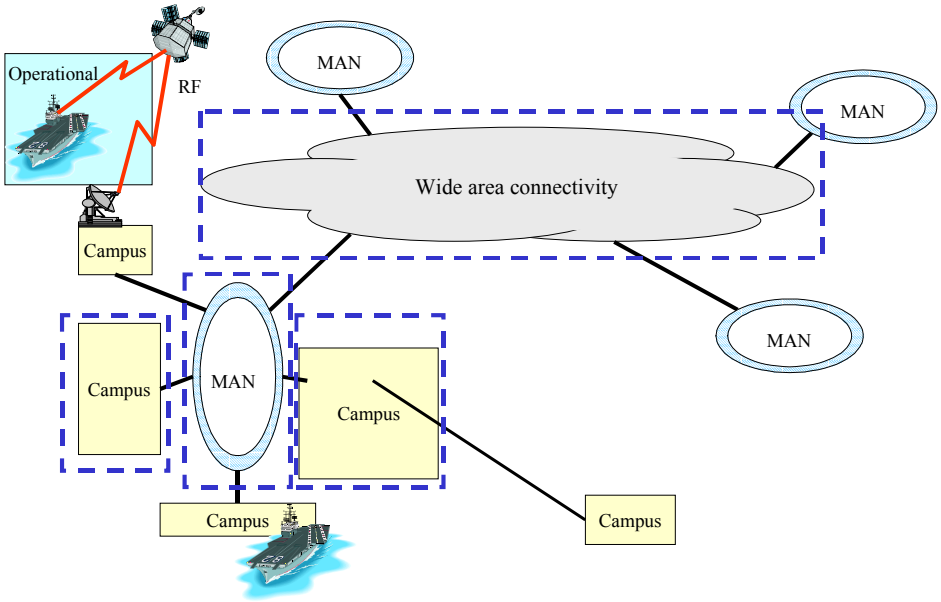

Figure 2-1. End-to-End Network Connectivity

The specific inter-network connectivity requirements are summarized in the following four sub-sections for each of the four network categories.

2.3.1 Operational Area Network Connectivity Requirements

There is a requirement to optimize operational area services to enable a solution to the fleet mobility problem and to enable the fleet intranet. The Operational Area Network connectivity requirements include:

- Military satellite communications
- Commercial satellite communications
- Communication link system
- COMSECURITY system
- Military line-of-sight communications
- Commercial line-of-sight systems
- Communication transceivers
- Communication Umbilical System
- Fleet Teleport System
- Communication Antenna System
- Pier interface

2.3.2 Campus Area Network Connectivity Requirements

There is a requirement within the campus area network to optimize campus area services. The CAN connectivity requirements are:

- Campus Area Network
- Campus Area Network/Local Area Network interfaces
- Campus Area Network/Metropolitan Area Network interfaces
- Campus Area Network/Wide Area Network interfaces

2.3.3 Metropolitan Area Network Connectivity Requirements

There is a requirement within the metropolitan area network to optimize the provisioning of metropolitan area services in areas of high concentration of DON and joint campuses. The MAN requirements are:

- Metropolitan Area Network
- Metropolitan Area Network/Local Area Network interfaces
- Metropolitan Area Network/Campus Area Network interfaces
- Metropolitan Area Network/Wide Area Network interfaces

2.3.4 Wide Area Network Connectivity Requirements

There is a requirement within the wide area network to optimize wide area services. The WAN requirements are:

- Wide Area Networks
- DISN
    - NIPRNET
    - SIPRNET
- Internet
- Commercial telephone
- Secure commercial telephone
- Defense Switched Network (DSN) access
- Wide Area Network/Local Area Network interfaces
- Wide Area Network/Campus Area Network interfaces
- Wide Area Network/Metropolitan Area Network interfaces
- Wide Area Network to external network interfaces